UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/606,659	06/25/2003	Bing Wang	08212/0200290-US0/NC28834	4744

53666   7590   10/27/2008
BRAKE HUGHES BELLERMANN LLP
c/o INTELLEVATE
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER
OKEKE, IZUNNA

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
10/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _25 June 2003_.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-43_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-43_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _25 June 2003_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _03/27/2008_.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1.   Applicant's arguments with respect to claims 1-43 have been considered but are moot in

view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

2.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3.   Claims 1-32 and 33-43 are rejected under 35 U.S.C. 102(b) as being anticipated by

Waldin et al. (US-6094731).

a.   *Referring to amended claim 1:*

Regarding amended claim 1, Waldin teaches a method for filtering out exploits passing

through a device (See Abstract), comprising:

receiving an object to be inspected directed to the device (Col 5, Line 51-52 teaches the recipient

receiving a file);

determining a first hash value associated with the object to be inspected (Col 6, Line 18-21

teaches determining a first hash value which is a hash of the size of the file);

determining a second set of hash values associated with objects that have previously been

scanned (Col 6, Line 18-21 teaches determining a second set of values which is a hash of the size

of the file that has been previously stored);

if the first hash value matches at least one of the hash values in the second set, determining a

third hash value associated with the object to be inspected (Col 6, Line 18-21 teaches comparing

the hashes of the size of the file and Col 6, Line 37-42 teaches if they match, then determining a

hash of the sectors of the file);

determining a fourth set of hash values associated with the objects that have previously been

scanned (Col 6, Line 37-42 teaches determining the pre-stored hash of the sectors of the file);

and

if the third hash value matches at least one of the hash values in the fourth set, immediately

processing the object to be inspected (Col 49-52 teaches if the hash of the sector matches the pre-

stored values, then immediately processing the file without scanning the file for virus).

a.   *Referring to claim 4:*

        Regarding claim 4, Waldin teaches the method of Claim 1, wherein the first hash value

includes a rough outline hash value (ROHV) (Col 4, Line 63-65 teaches a hash of the size of the

file as the ROHV).

a.   *Referring to claim 5:*

        Regarding claim 5, Waldin teaches the method of Claim 4, wherein the third hash value

includes a sophisticated signature hash value (SSHV) and wherein the ROHV requires less time

to compute than the SSHV (Col 4, Line 58-60 teaches the hash of the sectors of the file as the

SSVH which requires more time to compute than the ROHV).

a.   *Referring to amended claim 6:*

        Regarding amended claim 1, Waldin teaches the method of Claim 1, wherein

immediately processing the object further comprises forwarding the object to be inspected to an

output component without scanning the object to be inspected (Col 6, Line 49-67 and Col 7, Line

1-3 teaches forwarding the file to the user or intended recipient without scanning the file if the comparison of the hash of the sectors match).

a.   *Referring amended to claim 8:*

Regarding amended claim 8, Waldin teaches the method of Claim 6, wherein immediately processing the

object to be inspected further comprises forwarding the object to be inspected to a destination (Col 6, Line 49-67 and Col 7, Line 1-3 teaches forwarding the file to the user or recipient without scanning the file if the comparison of the hash of the sectors match).

a.   *Referring amended to claim 9:*

Regarding amended claim 9, Waldin teaches the method of Claim 1, further comprising if the first hash value does not match any of the hash values in the second set, scanning the object to be inspected for an exploit; and updating the second set of hash values to include the first hash value (See Col 6, Line 21-25).

a.   *Referring to amended claim 10:*

Regarding amended claim 10, Waldin teaches the method of Claim 1, further comprising if the third hash value does not match any of the hash values in the fourth set, scanning the object to be inspected for an exploit; and updating the fourth set of hash values to include the third hash value (See Col, Line 42-45).

a.   *Referring to amended claim 12:*

Regarding amended claim 12, Waldin teaches a computer storage medium encoded with a data-structure (See Col 3, Line 46-56), comprising:

a first indexing data field having indexing entries, each indexing entry including a first hash

value (See Fig 1, Size F(1)); and

a second data field including object-related entries, each object-related entry having a second

hash value and being indexed to an indexing entry in the first indexing data field (See Fig 1, Size

F(1) on recipient computer), each object-related entry being uniquely associated with an object

that has been previously scanned (See Fig 1, the file related entry are associated with File 1).

a.   *Referring to amended claim 14:*

Regarding amended claim 14, Waldin teaches the computer storage medium of Claim 12,

wherein the first hash value is a rough outline hash value (ROHV) (See the rejection in claims 1

and 12).

a.   *Referring to amended claim 15:*

Regarding amended claim 15, Waldin teaches the computer storage medium of Claim 12,

wherein the second hash value is a sophisticated signature hash value (SSHV) (See the rejection

in claims 1 and 12).

a.   *Referring amended to claim 16:*

Regarding amended claim 16, Waldin teaches the computer storage medium of Claim 12,

wherein at least one object-related entry in the second data field includes information about the

associated object See the rejection in claim 12).

a.   *Referring to amended claim 17:*

Regarding amended claim 17, Waldin teaches a system embodied on a computer storage

medium encoded with a data-structure for protecting a device against an exploit Col 3, Line 47-

67 and Col 4, Line 1-3), comprising:

a message tracker that is configured to determine whether an object has been previously scanned

using a two-phase hash value technique (See Fig 1 and Col 6, Line 18-50 teaches the Antivirus

accelerator module 5' determines if the object has been previously scanned using the two-phase

technique); and

a scanner component that is coupled to the message tracker and that is configured to receive an

unscanned object and to determine whether the unscanned object includes an exploit (See Fig 1

and Col 6, Line 18-50 teaches the Antivirus scan module as the scanner module which receives

instruction from the accelerator module to scan the file if it includes an exploit).

a.   _Referring to claim 19:_

        Regarding claim 19, Waldin teaches the system of Claim 17, wherein the two-phase hash

value technique comprises:

determining a first hash value associated with the object (See the rejection in claims 1 and 17);

determining a second set of hash values associated with objects that have previously been

scanned (See the rejection in claims 1 and 17); and

if the first hash value does not match at least one of the hash values in the second set,

determining that the object has not been previously scanned (See Col, Line 37-39 teaches that the

file is either infected or unscanned if the size hash doesn't match).

a.   _Referring to claim 21:_

        Regarding claim 21, Waldin teaches the system of Claim 19, wherein the first hash value

further comprises a ROHV (See the rejection in claims 1 and 19).

a.   _Referring to claim 22:_

        Regarding claim 1, Waldin teaches the system of claim 19, wherein the two-phase hash

value technique further comprises:

if the first hash value matches at least one of the hash values in the second set, determining a

third hash value associated with the object (See the rejection in claims 1 and 19);

determining a fourth set of hash values associated with the objects that have previously been

scanned (See the rejection in claims 1 and 19 teaching the pre-stored values as the hash values

associated with the file);

if the third hash value does not match at least one of the hash values in the fourth set,

determining that the object has not been previously scanned.

a.   *Referring to claim 24:*

        Regarding claim 24, Waldin teaches the system of Claim 22, wherein the third hash value

further comprises a SSHV (See the rejection in claims 1 and 22).

a.   *Referring to claim 25:*

        Regarding claim 25, Waldin teaches the system of Claim 22, wherein the two-phase hash

value technique further comprises:

if the third hash value approximately matches at least one of the hash values in the fourth set,

determining that the object has been previously scanned (Col 6, Line 43-46 teaches if the sectors

hash value doesn't match the pre-stored values, then the file is either infected or unscanned at

which point the scan module scans it again).

a.   *Referring to claim 30:*

        Regarding claim 30, Waldin teaches the method of Claim 1, wherein: the first hash value

and third hash value are determined by the device (Col 6, Line 10-55 teaches the first and third

hash values are determined by the device); and

the second set of hash values and the fourth set of hash values are determined by the device

based on previous scanning by the device (Col 6, Line 10-55 teaches the second and the fourth

hash values are pre-stored values or hashes of previous scans).

a.   *Referring to claim 31:*

Regarding claim 31, Waldin teaches the method of claim 1, wherein the method is

performed by a firewall (Col 3, Line 21-28)

a.   *Referring to claim 32:*

Regarding claim 32, Waldin teaches the method of claim 1, wherein the method is

performed by a router (Col 3, Line 21-28).

a.   *Referring to claim 34:*

Regarding claim 34, Waldin teaches the system of claim 17, wherein the system includes

a firewall (Col 3, Line 21-28).

a.   *Referring to claim 35:*

Regarding claim 35, Waldin teaches the system of claim 17, wherein the system includes

a router (Col 3, Line 21-28).

a.   *Referring to claim 36:*

Regarding claim 36, Waldin teaches a method comprising: receiving an object; matching

a rough outline hash value (ROHV) of the object to ROHVs of known objects; if a match is

found between the ROHV of the object to any of the ROHVs of the known objects, matching a

sophisticated signature hash value (SSHV) of the objects to SSHVs of the known objects;

if a match is found between the SSHV of the object to any of the SSHVs of the known objects,

processing the object as a malicious object;

if a match is not found between either the ROHV of the object to any of the ROHVs of the

known objects or the SSHV of the object to any of the SSHVs of the known objects, scanning

the object; and

if the scanning the object determines that the object is malicious, processing the object as a

malicious object and updating the ROHVs of known objects and the SSHVs of the known

objects (Col 6, Line 17-55 teaches a receiving a file, comparing the ROHV (size) to a stored

value, if a match is found, comparing the SSHV (hash of sectors) to stored values and processing

the object is a match is found or scanning the file if a match is not found).

a.   *Referring to claim 37:*

        Regarding claim 37, Waldin teaches the method of claim 1, wherein the determining the

first hash value includes determining a rough outline hash value (ROHV) based on a hash value

of a first portion of the object (See the rejection in claim 1).

a.   *Referring to claim 38:*

        Regarding claim 38, Waldin teaches the method of claim 37, wherein determining the

third hash value includes determining a sophisticated signature hash value (SSHV) based on a

Message Digest 5, a Secure Hash Algorithm, or a Secure Hash Standard, and wherein the ROHV

requires less time to compute than the SSHV (Col 1, Line 41-47 teaches common hash functions

known in the art such as MD5, SHA-1 used in forming a hash of the file which requires more

time to compute than the hash of the size).

a.   *Referring to amended claim 39:*

        Regarding amended claim 39, Waldin teaches the computer storage medium of Claim 12,

wherein the first hash value is a rough outline hash value (ROHV) determined based on a hash

value of a first portion of the object (See the rejection in claim 12 and 37).

a.   *Referring to amended claim 40:*

Regarding amended claim 40, Waldin teaches the computer storage medium of Claim 12,

wherein the second hash value is a sophisticated signature hash value (SSHV) determined based

on a Message Digest -5, a Secure Hash Algorithm, or a Secure Hash Standard (See the rejection

in claims 12 and 38).

a.   *Referring to claim 41:*

Regarding claim 41, Waldin teaches the system of Claim 19, wherein the first hash value

further comprises a ROHV determined based on a hash value of a first portion of the object (See

the rejection in claim 1).

a.   *Referring to claim 42:*

Regarding claim 42, Waldin teaches the system of Claim 22, wherein the third hash value

further comprises a SSHV determined based on a Message Digest -5, a Secure Hash Algorithm,

or a Secure Hash Standard (See the rejection in claims 1 and 38).

a.   *Referring to claim 43:*

Regarding claim 43, Waldin teaches The method of claim 36, wherein: the ROHV is

determined based on a hash value of a first portion of the object; and the SSHV is determined

based on a Message Digest -5, a Secure Hash Algorithm, or a Secure Hash Standard See the

rejection in claims 1, 37 and 38).

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
manner in which the invention was made.

5.   Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Waldin et al.

(US-6094731), and further in view of Chen et al. (US-5960170)

a.   *Referring amended to claim 33:*

Regarding claim 33, Waldin teaches the method of claim 1.

Waldin does not teach determining whether the file is compressed and if it is,

decompressing the file.

However, Chen teaches determining if the object is compressed and decompressing the

object if it is (See Chen, Col 15, Lines 5-13)

Therefore, it would have been obvious to one of ordinary skill at the time the invention

was made to modify Waldin's system to determine if the file is compressed and to decompress it

as taught by the Chen for the purpose of making the system more efficient in processing large

files which have been compressed to a smaller size.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to IZUNNA OKEKE whose telephone number is (571)270-3854.

The examiner can normally be reached on 9:00am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. O./
Examiner, Art Unit 2432

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2432